California Dental Association
Practice Support
800.232.7645 cda.org/practicesupport

HIPAA Security Rule - A Summary

Congress passed the Health Insurance Portability and Accountability Act in 1996 to simplify, and thereby reduce the cost of the administration of health care. HIPAA does this by encouraging the use of electronic transactions between health care providers and payers, thereby reducing paperwork. Congress deemed that if the electronic transmission of patient health information was to be encouraged by the legislation, there needed to be means to protect the confidentiality of that information. The HIPAA Privacy Rule, which had a compliance date of April 14, 2003, is the first regulation to establish standards for the protection of patient health information. The Security Rule, with a compliance date of April 21, 2005, focuses specifically on standards to protect the confidentiality of electronically transmitted patient information.

California Confidentiality of Medical Information Act

State law imposes requirements similar to the HIPAA Security Rule on all health care providers. This includes providers who do not conduct electronic transactions or undertake other activities that would designate them as HIPAA covered entities. Compliance with the HIPAA Security Rule makes compliance with the CMIA security provisions simple. The Office of Health Information Integrity (OHII) provides information about the law.

The state requires that *if electronic recordkeeping systems are only utilized* in the dental office, the office must use an offsite backup storage system, an image mechanism that is able to copy signature documents, and a mechanism to ensure that once a record is input, it is unalterable. The dentist must develop and implement policies and procedures to include safeguards for confidentiality and unauthorized access to electronically stored record, authentication by electronic signature keys, and systems maintenance. The electronic health record system must automatically record and preserve any change or deletion of electronically stored health information and requires the record to include, among other things, the identity of the person who accessed and changed the information and the change that was made to the information.

HIPAA Privacy and Security Rules: The Similarities, the Differences

Implementation of the HIPAA Privacy Rule requirements is eased by the flexibility of the regulatory standard within the rule. The Privacy Rule compliance standards for regulated entities (i.e., health care providers who conduct certain transactions electronically) include reasonable measures to protect the confidentiality of patient information. What constitutes reasonable measures for a particular practice are largely determined by such things as the size of the practice, the physical layout of the office, how patient information is used and conveyed within the practice, even such factors as cost. What might be a reasonable measure to protect patient information within a hospital setting is going to be different from a reasonable measure in a dental practice with one or two dentists. Measures that are reasonably necessary for a hospital to protect against the unauthorized release of patient information are likely going to be unreasonable for a small private practice.

The standard of compliance for the Security Rule is the same: the regulated entity must install reasonable measures to secure patient information. What are reasonable security measures for a large entity like a hospital are likely to be unreasonable for a small entity like a private dental practice. There is also some overlap between the requirements of the Privacy Rule and the Security Rule, meaning that what a dental practice did to comply with the Privacy Rule ensures

that the practice is already in partial compliance with the Security Rule.

There are differences between the concepts of privacy and security, however. Privacy deals with what might be termed "leakage" of protected personal health information. Such leakage occurs and can be controlled by how patient files are used, how they are moved through the office during the day, and whether they are ever left in a place where they might be accessible to other patients. Leakage also deals with where conversations take place with patients about their oral health condition, discussions about recommended treatment of their condition, and conversations about how they will be paying for that treatment. Obviously, such conversations should not take place in the office waiting room or reception area, or within earshot of other patients.

Whereas the Privacy Rule protects against leakage of protected information, the Security Rule deals with unauthorized invasion of confidential patient records or interception of electronic transmissions. The scope of the rule addresses the protection of patient information that has been electronically created or stored. In this regard, the Security Rule does not address patient information that is in a written document or communicated orally. The focus of the Security Rule is to protect against hackers breaching a computer network's firewall, the interception of viruses that are attached to emails, the use of passwords to ensure only authorized access to electronically stored patient information, protection against interception of electronic transmission patient information, and the like.

HITECH and Business Associates

Passage of the 2009 federal economic stimulus package included the Health Information Technology for Economic and Clinical Health Act (HITECH), which contains several modifications to HIPAA guidance and regulations. The new act expands the responsibility of covered entities and business associates in securing the privacy of health information.

HITECH mandates business associates comply with the HIPAA Security Rule and makes them subject to the same civil and criminal penalties as covered entities. Previously, business associates were only contractually obligated to comply with HIPAA through agreements with covered entities. For information on business associates and business associate agreements, refer to the resource, *HIPAA Business Associate Agreement*, on cda.org/practicesupport.

Security Rule Requirements

In complying with the HIPAA Security Rule, covered entities and business associates should begin by recognizing three basic elements:

- Confidentiality. Ensure data or information is not made available or disclosed to unauthorized entities.
- Integrity. Ensure data or information is not altered by unauthorized entities.
- Availability. Ensure data or information is accessible and usable upon demand by an authorized entity.

Covered entities and business associates must comply with the Security Rule standards that are categorized as follows: administrative safeguards, physical safeguards, and technical safeguards. Essentially, **administrative safeguards** involve documented, formal practices to manage the selection and implementation of security measures; **physical safeguards** control physical access to information systems, especially at times when there is a loss of power or natural disaster; and **technical safeguards** involve processes that protect and monitor information access, and protect data that is transmitted over a network.

Many of the compliance standards include implementation specifications. The implementation specifications are either "required" or "addressable." Required specifications must be implemented. Addressable specifications should be implemented if the business, after it conducts its risk analysis, deems the specification reasonable, appropriate and applicable. Where there is no implementation specification for a standard, compliance with the standard itself is required.

Required administrative safeguards include:

- conducting thorough initial and periodic analyses to determine potential risks to the security of patient information that is stored and used electronically;
- implementing practices to reduce identified risks and vulnerabilities;
- instituting a system to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports;
- responding to security incidents;
- training staff (including unpaid volunteers and students who work in the practice) to be aware of and follow office information security policies and procedures;
- implementing a policy to sanction staff members who violate office information security policies and procedures;
- designating one staff person to be the Security Officer (similar to the designation of a Privacy Officer as required by the HIPAA Privacy Rule);
- establishing appropriate access levels for staff to patient records (determined by job requirements);
- assigning a unique name and/or number for identifying and tracking identity of information system users;
- establishing data backup and disaster recovery plans;
- establishing contingency plan to enable continuation of critical business processes for protection of the security of patient information while operating in emergency mode; and
- having business associate agreements that require compliance with Security Rule and notification of data breaches that occur with the respective business associate

Addressable administrative safeguards include:

- implementing procedures for the authorization and/or supervision of staff members who work with patient information or in locations where it might be accessed;
- implementing procedures to determine that the access of a staff member to patient information is appropriate;
- implementing procedures for terminating access to patient information when employment of a staff member ends;
- implementing security reminders;
- implementing procedures to guard against and detect malicious software
- implementing procedures for periodic testing and revision of contingency plans; and
- implementing procedures for creating, changing, and safeguarding passwords.

Required physical safeguards include:

- implementing policies and procedures to limit physical access to a practice's information system to authorized individuals for specified activities;
- implementing policies and procedures for workstation use that specify the functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings (includes tablets and PDAs)
- implementing policies and procedures to ensure the physical safeguard and security of workstations; and
- implementing policies and procedures governing receipt, security, transport, removal, re-use, and disposal of

hardware and electronic media containing electronically stored protected health information.

Addressable physical safeguards include:

- establishing procedures that allow access to the physical space where data is stored in support of restoration of lost data under a disaster recovery plan and emergency mode operations plan;
- implementing policies and procedures to safeguard the physical facility and equipment from unauthorized physical access and theft;
- implementing procedures to verify a person's authorization to access facilities and software programs for testing and revision;
- implementing policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, walls, doors, and locks); and
- creating a retrievable, exact copy of patient information before equipment is moved from where it is stored.

Required technical safeguards are:

- access controls, including unique user identification and emergency access procedure;
- audit controls (ability to monitor/track activity on the a practice's information system); and
- person or entity authentication.

Addressable technical safeguards are:

- automatic logoff (electronic procedures that terminate a session after a predetermined time of inactivity);
- implementing a mechanism to encrypt patient information whenever appropriate;
- implementing policies and procedures to prevent improper alteration of information on the system; and
- implementing mechanism to verify that patient information has not been altered or destroyed in an unauthorized manner.

Many of these safeguards have been added to current versions of practice management software. Dental offices should contact their practice management software vendors to inquire about the development and availability of upgraded versions that are compliant with HIPAA's Security Rule. Also, be aware that the security standards were written to be technology neutral, that is, use of specific technologies is not mandated so that entities are not bound by systems or software that may become obsolete.

Risk Analysis/Risk Management

Through its enforcement actions and audits, the U.S. Department of Health and Human Services (HHS) has identified the lack of, or an incomplete, risk analyses as a key factor in the failure of covered entities to adequately safeguard information. A risk analysis is a required administrative safeguard. It is intended to be an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the covered entity. "Risk" is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact. "Vulnerability" is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally or intentionally) and result in a security breach or violation of security policy. Covered entities must evaluate the risk levels and, for high risk items, describe how the risk is mitigated or how it will be managed.

The ADA Practical Guide to HIPAA Compliance (2013) includes a dental practice-specific risk assessment tool. Also, HHS offers a risk assessment tool online. The link to the tool is listed under Resources below. Be sure to read the user's

guide and watch the videos that accompany the tool in order to understand the scope of work required.

Flexibility of Approach

It bears repeating that HIPAA allows covered entities flexibility in reasonably and appropriately implementing safeguards. The regulation states:

> § 164.306 Security standards: General rules.
> (a) General requirements. . . .
> (b) Flexibility of approach.
> (1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
> (2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors:
> (i) The size, complexity, and capabilities of the covered entity or business associate.
> (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.
> (iii) The costs of security measures.
> (iv) The probability and criticality of potential risks to electronic protected health information.
> (c) Standards. . . . ..

For further information on the Security Rule, or other HIPAA requirements, contact CDA Practice Support, 800.232.7645, or practicesupport@cda.org.

Resources

American Dental Association
Security Rule Guidance Material, US Department of Health and Human Services
HHS Security Risk Assessment Tool
HIPAA for Covered Entities and Business Associates, US Department of Health and Human Services
Guide to Storage Encryption Technologies for End User Devices, NIST Special Publication 800-111
NIST, Computer Security Incident Handling Guide
Mobile Devices and Health Information Privacy and Security, US Department of Health and Human Services
California Office of Health Information Integrity (OHII)

On cda.org/practicesupport:

HIPAA and California Health Information Privacy and Protection Laws Q&A
HITECH Act/Omnibus Rule Revises Certain HIPAA Provisions
Data Breach Notification Requirements Checklist
Patient Records: Requirements and Best Practices